Business Requirements Document (BRD)

Project: User Authentication System Implementation

1. Executive Summary

The project aims to implement a secure, efficient user authentication system within the existing web application. This will enable users to register, log in, and manage their profiles securely, while supporting future functionality related to access control and user roles.

2. Background and Current State

Currently, the web application allows anonymous access to all features, which restricts the ability to personalize the user experience and compromises data security. This lack of authentication and authorization results in data access issues and limits the app's ability to support user-specific features.

3. Objectives

- To secure user data by requiring authentication.

- To allow registered users to access personalized content and settings.

- To support future features such as role-based access control.

4. Scope

The scope includes:

- User registration, login, logout, and password recovery.

- Profile management (update email, password, profile details).

- Password encryption and basic account security measures.

Out of Scope:

- Two-factor authentication (TFA) and social login options.

- Role-based access control beyond simple user/admin roles.

5. Functional Requirements

- FR1: Users should be able to register with a unique email and password (High).

- FR2: Users should be able to log in using registered credentials (High).

- FR3: Users should be able to reset their password via email verification (High).

- FR4: Users should be able to log out from the system securely (Medium).

- FR5: System should validate passwords for a minimum of 8 characters (Medium).

- FR6: Users should be able to update their email, password, and profile info (Medium).

6. Non-Functional Requirements

- NFR1: The authentication system should respond within 2 seconds (High).

- NFR2: User data should be stored securely with encryption (High).

- NFR3: The system should handle at least 10,000 concurrent login requests (Medium).

- NFR4: Session management should maintain security without impacting performance (Medium).

7. Assumptions

- Users have unique email addresses.

- The application is hosted on a secure server.

8. Risks and Mitigations

- Risk: Potential delays due to integration with the current database.

- Mitigation: Allocate additional time for database schema changes.

9. Success Criteria

- Users can register, log in, and manage profiles.

- Sensitive data is encrypted.

- Authentication system passes performance testing with expected load.

10. Appendix

- Glossary of Terms

- Relevant Diagrams (e.g., use case or sequence diagrams)